РОЗДІЛ 8
КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.85
DOI https://doi.org/10.32782/2524-0374/2020-4/59

ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

CRIME PREVENTION IN THE FIELD OF INFORMATION TECHNOLOGIES: INTERNATIONAL AND LEGAL ASPECT

Бодунова О.М., к.ю.н.,
доцент кафедри кримінального права та кримінології
Університет державної фіскальної служби України

У статті розглядається досвід зарубіжних країн, зокрема США, Канади, Франції, щодо запобігання злочинності у сфері інформаційних технологій.

Зауважено, що поширення інформаційних технологій має негативні наслідки, адже відкриває шлях до злочинної поведінки. Комп'ютерні системи надають нові, дуже досконалі можливості для вчинення невідомих раніше правопорушень, а також для вчинення традиційних злочинів, але нетрадиційними засобами. Саме тому зробити дієвими чи вдосконалити реалізацію національних стратегічних підходів із розглядуваного питання можливо, лише спираючись на досвід позитивної діяльності урядових і поза державних організацій інших країн, а також міждержавних інституцій та враховуючи їх зрушення у запобіганні загрозам інформаційній безпеці.

Зазначено, що злочинність у сфері інформаційних технологій характеризується високим рівнем латентності. Це зумовлено складністю виявлення осіб, що вчиняють кримінальні правопорушення у сфері інформаційних технологій, відсутністю єдиної методики розслідування та сформованої системи запобігання даному виду злочинності.

Порівняльно-правовий аналіз законодавства зазначених вище країн і України дав змогу стверджувати, що там створена цілісна і розгалужена система державних органів та неурядових організацій, діяльність яких спрямована на запобігання злочинності у сфері інформаційних технологій. Такі органи наділені власними повноваженнями щодо запобігання злочинності у сфері інформаційних технологій, у результаті діяльності яких повністю реалізується система заходів запобігання даному виду злочинності. Зокрема, детально проаналізовано досвід Франції, у системі державних органів якої створено: відділ кіберзлочинів технічного обслуговування судових досліджень та документації; комп'ютерний і електронний відділ Інституту кримінального розслідування Національної жандармерії; відомчі бригади інформації та судових розслідувань (BDRIJ) тощо.

Звернено увагу на те, що актуальним для України є досвід Франції щодо запобігання злочинності у сфері інформаційних технологій, а саме забезпечення діяльності різних державних органів, кожен з яких має власні завдання (розслідування, запобігання, облік осіб, що вчинили дані кримінальні правопорушення, тощо).

Ключові слова: злочинність, кримінальні правопорушення, зарубіжний досвід, кримінальні правопорушення, запобігання, розкриття.

The article examines the experience of foreign countries, in particular, the United States, Canada, France, in the prevention of crime in the field of information technology.

It is noted that the spread of information technology has negative consequences, because it opens the way to criminal behavior. Computer systems provide new, very advanced opportunities to commit previously unknown offenses, as well as to commit traditional crimes, but by unconventional means. That is why it is possible to make effective or improve the implementation of national strategic approaches to this issue only based on the experience of positive activities of governmental and non-governmental organizations of other countries and intergovernmental institutions and taking into account their progress in preventing information security threats.

It is noted that crime in the field of information technology is characterized by a high level of latency. This is due to the difficulty of identifying persons committing criminal offenses in the field of information technology, the lack of a unified methodology of investigation and the established system of prevention of this type of crime.

A comparative legal analysis of the legislation of the above countries and Ukraine allowed us to state that there is a holistic and extensive system of government agencies and non-governmental organizations whose activities are aimed at preventing crime in the field of information technology. Such bodies are endowed with their own powers to prevent crime in the field of information technology, as a result of which the system of measures to prevent this type of crime is fully implemented. In particular, the experience of France is analyzed in detail, in the system of state bodies of which the following has been created: the Department of Cybercrime, Maintenance of Judicial Research and Documentation; computer and electronic department of the Institute of Criminal Investigation of the National Gendarmerie; departmental information and judicial investigation teams (BDRIJ), etc.

Attention is drawn to the fact that the experience of France in preventing crime in the field of information technology is relevant for Ukraine, namely ensuring the activities of various government agencies, each of which has its own tasks (investigation, prevention, registration of perpetrators, etc.).

Key words: crime, criminal offenses, foreign experience, criminal offenses, prevention, disclosure.

Сьогодні суспільство переживає стрімкий розвиток автоматизації, інформатизації та комп'ютеризації кожної зі сфер діяльності. Ці процеси надають нові можливості для розвитку культури, освіти, науки й економіки кожної держави, а також дають змогу оперативно взаємодіяти з іншими державами та міжнародними організаціями. Проте поширення інформаційних технологій має й негативні наслідки, адже відкриває шлях до злочинної поведінки. Комп'ютерні системи надають нові, дуже досконалі можливості для вчинення невідомих раніше правопорушень, а також для вчинення традиційних злочинів, але нетрадиційними засобами.

Із цього приводу науковці М.В. Карчевський і В.В. Невгад правильно зазначають, що «кіберзлочинність», «кібершахраї», «хакери», «комп'ютерний злом», «крадіжка машинного часу» – це терміни, які перестали

бути «чимось недосяжним». Сьогодні злочинність у сфері інформаційних технологій – одна з найдинамічніших груп суспільно небезпечних посягань. Беззаперечним є те, що швидке збільшення рівня поширеності такої злочинності, а також постійне зростання її суспільної небезпеки стало зворотним, негативним явищем такого суспільно важливого процесу, як інформатизація.

Окрім того, злочинність у сфері інформаційних технологій характеризується високим рівнем латентності. За різними оцінками, правоохоронним органам стає відомо лише про 10–20% таких кримінальних правопорушень [1]. Усе це зумовлено складністю виявлення осіб, що вчиняють кримінальні правопорушення у сфері інформаційних технологій, відсутністю єдиної методики розслідування та сформованої системи запобігання даному виду злочинності.

Повністю погоджуючись із думкою О.В. Таволжанського, зазначимо, що зробити дієвими чи вдосконалити реалізацію національних стратегічних підходів із розглядуваного нами питання можливо, лише спираючись на досвід позитивної діяльності урядових і поза державних організацій інших країн, а також міждержавних інституцій та враховуючи їх зрушення у запобіганні загрозам інформаційній безпеці. У сучасних умовах складно уявити захищену державу, яка б не займалася власним секторами зовнішньої безпеки, змінюючи їх відповідно до викликів сучасності. Жодна війна, відкрита чи прихована, не відбувається без використання кіберзброї, потенціалу використання мережі Інтернет як кіберресурсу у військових цілях поза конкуренцією. Повсякденно в політиці провідних держав розробляються новітні заходи протидії загрозам у кіберпросторі, здійснюється коригування внутрішньої інформаційної політики, а також удосконалюються методи кібербезпеки [2, с. 155]. Саме це й зумовило актуальність дослідження злочинності у сфері інформаційних технологій та необхідності запобігання цьому негативному явищу.

Кримінологічні дослідження зарубіжного досвіду запобігання злочинності у сфері інформаційних технологій проводилися такими вченими, як П.Д. Біленчук, Л.Д. Варунц, М.І. Малій, В.В. Марков, О.В. Таволжанський та ін.

Досліджуючи дане питання, ми звернулися до досвіду найбільш розвинутих країн світу. Порівняльно-правовий аналіз законодавства цих країн і України дає змогу стверджувати, що за кордоном у більшості держав створено цілісну систему органів щодо забезпечення кібербезпеки. Так, у США, до таких органів можна віднести Управління національної безпеки (Department of Homeland Security), при якому здійснює свою діяльність спеціальний кібербезпекововий департамент, що займається виключно безпекою високотехнологічних систем США. Кіберкомандування очолює підрозділи спеціального призначення, які мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування і «обвал» структур супротивника з використанням можливостей кіберпростору.

У Канаді запобіганням комп'ютерним і телекомунікаційним кримінальним правопорушенням займається підрозділ Королівської канадської кінної поліції (далі – КККП). Діяльність підрозділу спрямована на розслідування та розкриття кримінальних правопорушень, пов'язаних із комп'ютерною діяльністю і телекомунікаціями. Секція захисту інформаційних технологій забезпечує захист федеральних державних комп'ютерних центрів, приватного сектору, надає консультації, готує персонал для роботи зі здійснення комп'ютерного захисту. Співробітники підрозділу допомагають поліцейським у проведенні розслідувань кримінальних правопорушень, пов'язаних із комп'ютерними системами. Ураховуючи, що інформаційна система дає змогу передавати повідомлення від одного терміналу до іншого майже негайно, у Канаді діє близько 2 500 точок доступу, до яких входять близько 1 285 федеральних і провінційних поліцейських відділень. 1 180 підрозділів спеціалізованих відділівКККП підключені до ліній системи [3, с. 127].

Безперечно, цей напрям діяльності поліції є важливим, оскільки економічні втрати вже досягли великих масштабів, деякі злочинці діють на міжнародному рівні у складі організованих груп. Одному державному органу складно запобігати злочинності у сфері інформаційних технологій.

У зв'язку із цим кримінологи стверджують, що канадське законодавство щодо визначення злочинності у сфері інформаційних технологій є суперечливим і потребує вдосконалення. Ураховуючи, що завдання, які стоять перед підрозділами поліції з боротьби зі злочинністю у сфері інформаційних технологій, носять міжнародний характер і не є специфічними для Канади, вони активно співпрацюють з іншими країнами та Інтерполом із метою вдосконалення законодавства у цьому напрямі. Розкриття комп'ютерних кримінальних правопорушень є складним завданням передусім через фактор часу. Оскільки передача даних може бути виконана майже миттєво, часто буває даремно шукати будь-які докази, що підтверджують порушення міжнародного законодавства. За даними КККП, сьогодні безліч комп'ютерних кримінальних правопорушень здійснюється дітьми, які не досягли дванадцятирічного віку. Згідно з Кримінальним кодексом Канади, для встановлення кримінальної відповідальності необхідно довести несанкціоноване використання комп'ютерної системи та намір особи заподіяти своїми діями шкоду. Такий підхід потребує чіткого встановлення параметрів доступу до комп'ютерної техніки з метою попередження порушень. Необхідно враховувати дані про осіб, параметри доступу з урахуванням обмежень, можливість службовців «експериментувати» з програмами. Кваліфіковану консультацію щодо можливої неправомірної поведінки у цьому напрямі може надати міністерство юстиції чи відповідний підрозділ КККП [4, с. 110].

Слід зазначити, що методика розслідування випадків несанкціонованого дистанційного доступу до комп'ютерних мереж технічно складна, цим займаються спеціалізовані поліцейські підрозділи. З огляду на небезпеку комп'ютерної злочинності, тенденцію її розвитку та впливу на світове співтовариство, у межах ООН регулярно проводяться симпозіуми з профілактики і припинення комп'ютерної злочинності. Як один із напрямів фахівці відзначають програмні методи захисту інформації в комп'ютерних системах колективного користування шляхом удосконалення системи автоматичного контролю. На попередження та зменшення злочинів щодо незаконного використання телекомунікаційних систем на міжпровінційному, державному і міжнародному рівних спрямовані дії та управління боротьби з економічними злочинами. Допомагає поліцейським підрозділам Інформаційний центр [4, с. 110].

Аналізуючи досвід європейських країн, можемо зазначити, що як і в США, тут створено єдину систему державних органів, кожен з яких наділений окремими блоками повноважень щодо запобігання злочинності у сфері інформаційних технологій.

Так, у Франції створено низку державних інституцій та неурядових установ, що займаються запобіганням кіберзлочинності. Відомою є така структура, як Національна комісія з обчислювальної техніки та свобод (CNIL). Ціль діяльності CNIL – захисті персональних даних. У цифровому світі CNIL є регулятором персональних даних, підтримує фахівців у кіберпросторі в їхній діяльності і допомагає людям контролювати свої особисті дані та здійснювати свої права. З 2004 р. має право накладення санкцій на підприємства, що порушують Закон про інформатику, картотеки і свободи 1978 р. [5].

Окремим напрямом запобігання кіберзлочинності є діяльність так званого Верховного органу поширення творів і охорони прав в Інтернеті (HADOPI). Здійснена спроба визначити, що таке незаконне скачування інформації та регламентувати таку діяльність. Вищий конституційний суд країни схвалив другий варіант Закону про так звану триступеневу заборону доступу до мережі Інтернет [5].

У правоохоронній системі Франції також діють відповідні суб'єкти з боротьби зі злочинністю у сфері інформаційних технологій. Починаючи з 1998 р. Національна жандармерія визначила пріоритетною діяльність щодо вирішення проблем, пов'язану з інноваційними технологіями, шляхом створення відповідних структур і навчальних закладів, зокрема:

1. Відділ кіберзлочинів технічного обслуговування судових досліджень та документації (STRJD). Він здійснює моніторинг Інтернет-мережі шляхом пошуку злочинів проти людей та майна, пов'язаних із передачею нелегальних даних в Інтернеті (сайти, Інтернет-ресурси, групи новин, мережі обміну, соціальні мережі тощо).

2. Комп'ютерний і електронний відділ Інституту кримінального розслідування Національної жандармерії (IRCGN). Він розробляє методи, засоби та програмне забезпечення для автоматичного виявлення педофілів тощо.

3. Відомчі бригади інформації та судових розслідувань (BDRIJ) тощо.

Іншим суб'єктом запобігання кіберзлочинності у Франції є Національне агентство безпеки інформаційних систем (ANSII), французьке агентство з кібербезпеки, яке працює з державними спецслужбами. Діяльність органу спрямована на реалізацію Французької національної стратегії цифрової безпеки, оголошеної 16 жовтня 2015 р. Ця стратегія, що впроваджується ANSSI, є результатом скоординованих міжвідомчих зусиль, спрямованих на реагування на виникаючі проблеми цифрового століття. Було задекларовано, що цифровий перехід сприяє не лише інноваціям та економічному зростанню, а й одночасно несе ризики для держави, господарюючих суб'єктів та громадян. Кіберзлочинність, шпіонаж, пропаганда, саботаж та надмірне використання персональних даних загрожують цифровій довірі та безпеці. Визначено основні пріоритети в діяльності ANSSI: захист та безпека державних інформаційних систем та критично важливих інфраструктур, важливих операторів економіки та суспільства; цифрова довіра, конфіденційність, особисті дані, кібернасильство; підвищення обізнаності, початкове навчання, безперервна освіта; навколишнє середовище бізнесу цифрових технологій, промислова політика, експорт та інтернаціоналізація; цифрова стратегічна автономія, стійкість кіберпростору.

Доволі розповсюдженими сучасними заходами запобігання кіберзлочинності є проведення спільних навчань. У ході навчань виявляють недоліки, інфраструктури, формуються варіанти атак, інцидентів і пропонуються найбільш ефективні варіанти реагування та координації.

Cyber Europe-навчання передбачає симуляцію великих інцидентів із кібербезпеки, які загострюються, щоб стати кібернетичними кризами. Вправи пропонують можливості для аналізу передових технічних інцидентів кібербезпеки, а також для вирішення складних ситуацій безперервності бізнесу і кризових ситуацій. Навчання Cyber Europe показують сценарії з урахуванням реальних подій, розроблені європейськими експертами з кібербезпеки [6].

Отже, виходячи з вищесказаного, зазначимо, що у зарубіжних державах створено цілісну і розгалужену систему державних органів і неурядових організацій, діяльність яких спрямована на запобігання злочинності у сфері інформаційних технологій. Такі органи наділені власними повноваженнями щодо запобігання злочинності у сфері інформаційних технологій, у результаті діяльності яких повністю реалізується система заходів запобігання даному виду злочинності.

Уважаємо, що актуальним для України є досвід Франції щодо запобігання злочинності у сфері інформаційних технологій, а саме забезпечення діяльності різних державних органів, кожен з яких має власні завдання (розслідування, запобігання, облік осіб, що вчинили дані кримінальні правопорушення, тощо).

ЛІТЕРАТУРА

1. Малій М., Біленчук П. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? *Юридичний вісник.* URL : https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/ (дата звернення: 20.07.2020).

2. Таволжанський О.В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія «Право»*. 2018. № 6(18). С. 154–163.

3. Варунц Л.Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні : дис. … канд. юрид. наук : 12.00.07. Дніпропетровськ, 2012. 203 с.

4. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2(57). С. 107–113.

5. Loi favorisant la diffusion et la protection de la création sur Internet URL : http://www.senat.fr/dossier-legislatif/pjl07-405.html (дата звернення: 13.07.20120).

6. Loi 78-17 du 6 janvier 1978 modifiée. URL : https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978- modifiee (дата звернення: 13.07.2020).